(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－187007

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平9－347373

(22)出願日　平成９年(1997)12月17日

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号

(72)発明者　山北　徹
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

(74)代理人　弁理士　阪本　紀康

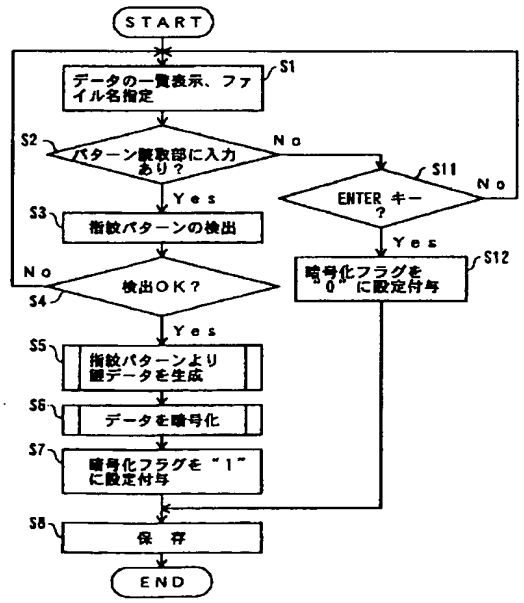
(54)【発明の名称】　暗号化・復号化装置およびその方法

(57)【要約】

【課題】　個人データのセキュリティが高く、且つ、そのデータの保存・取り出し操作が簡単である装置および方法を提供する。

【解決手段】　ユーザは、データを保存する際、自分の任意の指の指紋を暗号化装置に読み取らせる。暗号化装置は、読み取った指紋パターンに基づいて、鍵データを生成し、その鍵データを用いて保存すべきデータを暗号化する。暗号化されたデータを復号する際には、ユーザは、再度自分の指紋を読み取らせる。復号化処理では、復号化処理に際して読み取った指紋パターンに基づいて鍵データが生成され、その鍵データを用いてデータが復号される。

本実施形態の暗号化処理のフローチャート



1

【特許請求の範囲】
【請求項１】　パターン読取り手段と、
上記パターン読取り手段により読み取られた指紋パターンに基づいて暗号化の鍵データを生成する鍵データ生成手段と、
上記鍵データ生成手段により生成された鍵データを用いて対象データを暗号化する暗号化手段と、
を有する暗号化装置。
【請求項２】　上記パターン読取り手段により読み取られた指紋パターンに基づいて復号化の鍵データを生成する鍵データ生成手段と、
上記鍵データ生成手段により生成された鍵データを用いて上記暗号化手段により暗号化されたデータを復号する復号化手段と、
を有する請求項１に記載の暗号化装置。
【請求項３】　入力データを暗号化する方法であって、
ユーザの指紋パターンを読み取るステップと、
その読み取った指紋パターンに基づいて対象データを暗号化するステップと、読み取った指紋パターンに基づいて上記ステップにより暗号化されたデータを復号するステップと、
を有する暗号化方法。
【請求項４】　入力データを暗号化する処理を記述したプログラムを格納する記録媒体であって、
そのプログラムをコンピュータに実行させたときに
(a) ユーザの指紋パターンを認識する機能と、
(b) その認識した指紋パターンに基づいて対象データを暗号化する機能と、
(c) その認識した指紋パターンに基づいて上記機能により暗号化されたデータを復号する機能とを実現させる記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを暗号化・復号化する装置およびその方法に係わる。
【０００２】
【従来の技術】端末が互いに接続されたネットワーク環境下において、個人が管理するデータを他の人が容易に取り出せる状況下に有る。また、ネットワークのホスト機器などの機器を共有する場合に、他人に知られたくないデータを管理する必要性がある。このため、近年、文書や画像を始め、あらゆる種類の情報が電子化されている。そして、電子化された情報は、しばしば、他人に見られないように、あるいは改竄されないようにセキュリティがかけられている。
【０００３】現在、最も簡単で一般的なセキュリティ手法は、パスワードである。パスワードを用いたデータ保護では、よく知られているように、データをあるパスワードに対応付けて保存しておき、そのデータを格納するコンピュータ等は、そのデータに対する読出し指示を受

2

けると、ユーザにパスワードの入力を要求し、そのデータに対応付けられているパスワードが入力されたときのみそのデータを出力する。そして、このパスワードを個人または特定のグループに属する人のみが知るように管理し、他人に知られないようにすることにより、データへの不正アクセスを防いでいる。
【０００４】他のセキュリティ手法としては、暗号化が広く実施されている。暗号化は、データを所定のアルゴリズムに従って解読不能（意味不明）なデータに変換することにより、他人にそのデータの内容を知られないようにする技術である。暗号化アルゴリズムの中で最も一般的なものがＤＥＳ（Data Encryption Standard）である。暗号化アルゴリズムでは、上記ＤＥＳを始め、通常、暗号化・復号化のための鍵データ（暗号化キー、または、初期値等）が必要である。
【０００５】
【発明が解決しようとする課題】しかしながら、上述のような従来のセキュリティ手法においては、各ユーザがパスワード等を覚えておく必要があり、その負担が大きい。また、データを取り出す際、その都度パスワード等を入力する必要があり、手間がかかるという声も聞かれる。さらに、パスワード等が流出する恐れもある。この場合、パスワード等を定期的に変更することで対処することが多いが、このこともユーザの負担をさらに大きくしている。
【０００６】本発明の課題は、上述の問題を解決するものであり、データのセキュリティが高く、且つ、そのデータの保存・取り出し操作が簡単である装置および方法を提供することである。
【０００７】
【課題を解決するための手段】本発明の暗号化装置は、パターン読取り手段と、そのパターン読取り手段により読み取られた指紋パターンに基づいて暗号化の鍵データを生成する鍵データ生成手段と、その鍵データ生成手段により生成された鍵データを用いて対象データを暗号化する暗号化手段とを有する構成である。また、上記パターン読取り手段により読み取られた指紋パターンに基づいて復号化の鍵データを生成する鍵データ生成手段と、その鍵データ生成手段により生成された鍵データを用いて上記暗号化手段により暗号化されたデータを復号する復号化手段とをさらに設ける。
【０００８】上記構成によれば、データを暗号化する際に使用した指紋パターンと復号化する際に使用する指紋パターンとが互いに異なっていれば、上記暗号化手段により暗号化されたデータを上記復号化手段を用いて復号すると、解読不能または意味不明なデータが得られる。このことにより、データ作成者以外の他人にそのデータの内容を知られないようにしている。
【０００９】
【発明の実施の形態】以下、本発明の実施形態について

図面を参照しながら説明する。図１は、本発明の暗号化・復号化装置が適用される情報処理装置の一例として採り上げたパーソナルコンピュータの外観図である。パーソナルコンピュータ１は、ユーザの指示を入力するためのキーボード２、マウス３、およびディスプレイ４を備えると共に、物体の表面の凹凸パターンを検出するためのパターン読取部５を有する。パターン読取部５は、後述詳しく説明するが、本実施形態では、ユーザの任意の指の指紋パターンを読み取るために設けられている。

【００１０】図２は、本実施形態の情報処理装置の構成図である。記憶装置１１は、半導体メモリ、磁気的記録媒体、あるいは光学的記録媒体で構成され、プログラムおよびデータ等を格納している。記憶装置１１は、情報処理装置１に固定的に設けたものであってもよいし、着脱自在に装着するものであってもよい。

【００１１】記録媒体ドライバ１２は、可搬性記録媒体（半導体メモリ、磁気ディスク、光ディスク、光磁気ディスク等を含む）１３に格納されているデータを読み出したり、あるいは可搬性記録媒体１３にデータを書き込む装置である。通信制御部１４は、ネットワークとの間でのデータの授受を制御するユニットである。

【００１２】ＣＰＵ１５は、記憶装置１１または可搬性記録媒体１３からプログラム等をメモリ１６にロードして実行する。なお、後述する実施例で参照する各フローチャートの処理を記述したプログラム等は、たとえば、記憶装置１１にインストールされている。なお、そのプログラム等は、可搬性記録媒体１３に格納して供給することもできる。この場合、プログラム等は、記録媒体ドライバ１２を介してロードされる。また、そのプログラム等をネットワーク上の他の装置に格納しておき、それを通信回線を介して受信するようにしてもよい。更に、ＣＰＵ１５は、ネットワーク上に設けられた他の記憶装置に格納されているプログラムおよびデータ等を通信回線などを介して使用するようにしてもよい。

【００１３】パターン読取部５は、その表面に押圧された物体の表面の凹凸を検出する装置であり、微細化技術の進歩によりノード型パソコンに組み込むことができる程度に薄く形成されている。パターン読取部５は、たとえば、光源および２次元フォトセンサを含み、その２次元フォトセンサを構成する多数の受光素子がそれぞれ検出する受光レベルに対応する電流値または電圧値をシリアル形式またはパラレル形式で出力する。なお、本発明の出願人は、先に、十分に薄型でありながら高い精度で物体の表面の凹凸パターンを読み取ることができる読取装置について特許出願をしている（特願平９－２２２０１８号）。

【００１４】図３は、保存すべきデータを暗号化する処理のフローチャートである。このフローチャートの処理は、ユーザがデータを保存する旨の指示を入力したことをトリガとして実行される。なお、本実施形態の暗号化処理は、対象データの属性には依存せず、少なくともテキストデータ、表データ、画像データ、それらが混在したデータ、音声データに対して実行され得る。また、機械言語、高級言語で表わされたプログラムデータに対しても実行され得る。以下では、ファイル単位でデータを暗号化する例を示す。

【００１５】ステップＳ１では、保存すべき対象を認識する。この処理は、たとえば、データ一覧を表示し、その中からユーザにファイル名を指定させる手順を含んでもよい。ステップＳ２では、パターン読取部５に入力があったか否かを調べる。この処理は、たとえば、パターン読取部５の出力が変化したか否かを調べるものである。

【００１６】パターン読取部５に入力があった場合には、ユーザが所望の指の指先（指紋が形成されている部分）をパターン読取部５に押圧したものと見なし、ステップＳ３に進む。ステップＳ３では、指紋パターンを検出する。すなわち、パターン読取部５の出力を取り込む。ステップＳ４では、指紋パターンを適切に検出できたか否かを判断する。すなわち、ユーザの指がパターン読取部５に一定時間以上固定されなかった場合や、押圧が弱く接触面積が小さかった場合などには、指紋パターンを再生できないので、このステップで指紋パターンを適切に検出できたか否かを判断している。

【００１７】指紋パターンを適切に検出できた場合には、ステップＳ５において、その指紋パターンから鍵データ（暗号化キー等）を生成する。尚、本実施例では、暗号化アルゴリズムとして、ＤＥＳ（Data Encryption Standard）を採用するものとする。ＤＥＳは、６４ビットの入力を６４ビットの出力に変換するブロック暗号であり、この変換のために６４ビットの鍵データを使用する。６４ビットの鍵データのうち、８ビットはパリティとして使われる。本実施形態のステップＳ５は、この鍵データを生成するための処理であり、詳しくは後述する。

【００１８】ステップＳ６では、ステップＳ５で生成した鍵データを用いて保存すべきデータを暗号化する。ステップＳ７では、暗号化フラグを「１」に設定してそれを暗号化されたデータに付与する。そして、ステップＳ８において、暗号化されたデータと暗号化フラグとを対応づけて保存する。尚、データを保存する領域は、ユーザの指定に従い、例えば、記憶装置１１または可搬性記録媒体１３である。

【００１９】一方、ステップＳ２においてパターン読取部５に入力がなかっと判断した場合には、ステップＳ１１において、ＥＮＴＥＲキーが押圧されたか否かを調べる。ＥＮＴＥＲキーの押圧を検出した場合には、ステップＳ１２へ進み、暗号化フラグを「０」に設定して保存すべきデータに付与する。そして、ステップＳ３～Ｓ７をスキップし、ステップＳ８においてそのデータと暗号

化フラグとを対応づけて保存する。なお、ステップＳ１１において、ＥＮＴＥＲキーの押圧を検出できなかった場合には、ステップＳ１へ戻る。

【００２０】このように、本実施形態によれば、データを保存する際に所望の指の指紋パターンをパターン読取部５に読み取らせれば、ステップＳ３～Ｓ７が実行され、そのデータは指紋パターンに基づいて暗号化される。この操作は、非常に簡単であり、ユーザにとって負担とはならない。一方、データを保存する際にパターン読取部５に指紋パターンを読み取らせることなく、ＥＮＴＥＲキーを押圧すれば、ステップＳ３～Ｓ７がスキップされ、そのデータは暗号化されることなく平文のまま保存される。

【００２１】図４は、指紋パターンに基づいて鍵データを生成する処理のフローチャートである。この処理は、図３に示したフローチャートのステップＳ５を詳細に記載したものである。

【００２２】ステップＳ２１では、パターン読取部５により検出された指紋パターンデータをイメージデータに展開し、ノイズ除去などの前処理を施す。ステップＳ２２では、そのイメージデータから「線」を検出する。この処理は、たとえば、イメージデータ中の濃度が急激に変化する部分を「線」と見なすものであり、途切れた線を接続する処理や、線を直線または曲線に近似する処理を含む。

【００２３】ステップＳ２３では、検出した各線をそれぞれ指紋線（指紋パターンを形成する各線）とみなし、その指紋の渦の中心を検出する。ステップ２４では、指紋の渦の中心から数えて所定の数の指紋線を抽出する。ステップＳ２５では、抽出した各指紋線のパターンを曲線近似し、それら各曲線を表す方程式を導出する。ステップＳ２６では、各方程式に予め決められた所定の数を代入し、それら各解からそれぞれ所定のビット長のデータ列を生成する。そして、ステップＳ２７において、ステップＳ２６で生成したデータ列から鍵データを生成する。

【００２４】図５(a) は、暗号化処理の概念を示す図である。この図は、図３に示したフローチャートのステップＳ６の処理を概念的に示したものである。ＤＥＳによる暗号化処理では、入力データは、６４ビット毎に暗号化される。このとき、６４ビットの鍵データが使用される。すなわち、６４ビットの平文データＰおよび６４ビットの鍵データＫを関数Ｆに入力すると、６４ビットの暗号文データＣが得られる。関数Ｆは、ビット単位での転値処理を含み、所定回数繰り返し実行される。なお、ＤＥＳアルゴリズムは、その処理手順が公開されており、また、アルゴリズムそれ自体は本発明とは直接的には関係がないので、ここではその詳細な記載を省略する。

【００２５】次に、図３に示した処理に従って暗号化されたデータを復号する処理を説明する。本実施形態の復号化処理を示すフローチャートを図６に示す。このフローチャートの処理は、保存されているデータを読み出す旨の指示をユーザが入力したことをトリガとして実行される。

【００２６】ステップＳ３１では、ユーザが指定するアクセス先（記憶装置１１の所定のエリア、フロッピーディスク等）に保存されている読出し可能なデータの一覧を表示し、出力すべきデータをユーザに選択させる。ステップＳ３１において表示するデータ一覧の例を図７に示す。データ一覧は、保存されている各データのファイル名と、そのデータが暗号文として保存されているのか平文として保存されているのかを表示する。ここで、各データが暗号文として保存されているか平文として保存されているのかは、各データに付与されている暗号化フラグに従う。なお、ユーザは、マウス等を用いて所望のファイルを選択するものとする。

【００２７】ステップＳ３２は、図３に示したステップＳ２と同じであり、パターン読取部５に入力があったか否かを調べる。パターン読取部５に入力があった場合には、ステップＳ３３において、ステップＳ３１で選択されたデータが暗号化されているか否か調べる。すなわち、選択されたデータに付与されている暗号化フラグが「１」設定されているか否かを調べる。読み出すべきデータが暗号化されていた場合には、ステップＳ３４へ進む。

【００２８】ステップＳ３４およびＳ３５は、図３に示したステップＳ３およびＳ４と同じであり、指紋パターンを検出し、その検出が鍵データを生成するのに十分であったか否かを判断する。指紋パターンを十分に検出できたのであれば、ステップＳ３６においてその指紋パターンより鍵データを生成し、続いてステップＳ３７においてその鍵データを利用して暗号化されているデータを復号する。そして、ステップＳ３８において、その復号したデータを出力する。

【００２９】上記ステップＳ３６の処理は、図３に示したステップＳ５と全く同じであり、その詳細は図４に示した通りである。上記ステップＳ３７の処理は、基本的には図３に示したステップＳ６と同じであるが、若干異なる点がある。すなわち、暗号化と復号化とでは、鍵系列が互いに逆の順番で使用される。復号化処理の概念を図５(b) に示す。

【００３０】ステップＳ３２においてパターン読取部５に入力がなかっと判断した場合は、ステップＳ４１において、ＥＮＴＥＲキーが押圧されたか否か調べる。ＥＮＴＥＲキーの押圧を検出した場合には、ステップＳ４２へ進み、読み出すべきデータが暗号化されているか否か、すなわち、読み出すべきデータに付与されている暗号化フラグが「１」であるか否かを調べる。そして、読み出すべきデータが暗号化されていなかった場合には、

7

ステップＳ３８へ進み、そのデータを出力する。一方、読み出すべきデータが暗号化されていた場合、或いはステップＳ４１でＥＮＴＥＲキーが押圧されてないと判断した場合には、ステップＳ１へ戻る。

【００３１】上記構成によれば、ユーザの指紋パターンに基づいて暗号化されて記憶装置に格納されているデータを取り出す際、パターン読取部５に指紋パターンを読み取らせれば、ステップＳ３４～Ｓ３７が実行され、その暗号化されているデータはデータ取り出し時に読み取らせた指紋パターンに基づいて復号される。この時、暗号化する際に読み取らせた指紋パターンと復号化の際に読み取らせた指紋パターンとが互いに一致していれば、暗号化されているデータが正しく復号され、解読可能な状態に戻る。一方、上記２つの指紋パターンが互いに一致していなかった場合には、暗号化キーと復号化キーとが互いに異なることになるので、復号化処理が実行されたとしても、解読可能な平文を得ることはできない。すなわち、あるユーザの指紋パターンにより暗号化されたデータは、実質的に、そのユーザのみが解読できる状態に復号できることになり、セキュリティが守られる。

【００３２】なお、上記実施形態では、データを保存する際にそのデータを暗号化する構成を示したが、この処理は、新たに作成したデータを暗号化する場合、および以前に作成して保存してあったデータを取り出して再度保存する場合の双方に適用できる。また、この暗号化処理は、データの保存時のみでなく、データの転送時に行うこともできる。

【００３３】さらに、上記実施例では、暗号化アルゴリズムの１つとしてＤＥＳを採り上げて説明したが、本発明はこのアルゴリズムに限定されるものではない。例えば、疑似乱数を用いた暗号アルゴリズムにおいては、指紋パターンに従って疑似乱数発生器に与える初期値を生成するようにすればよい。

【００３４】なお、上記実施例では、データをファイル単位で保存もしくは転送する場合を示したが、データの所定の部分を暗号化する場合にも同様に実施できる。こ＊

8

＊の場合は、暗号化したい部分をマウス等で範囲指定し、指紋入力することによって範囲指定された部分を暗号化する。

【００３５】

【発明の効果】本発明によれば、従来のパスワード等の代わりに自分の指の指紋を使用して個人データのセキュリティを確保する構成なので、パスワード等を記憶・管理しておく必要がなく、また、流出の恐れもない。さらに、個人データの取り出し・保存の際に複雑な操作が不要になる。

【図面の簡単な説明】

【図１】本発明の暗号化・復号化装置が適用されるコンピュータの外観図である。

【図２】本実施形態の情報処理装置の構成図である。

【図３】本実施形態の暗号化処理のフローチャートである。

【図４】指紋パターンに基づいて鍵データを生成する処理のフローチャートである。

【図５】(a) および(b) は、それぞれ暗号化処理および復号化処理の概念を説明する図である。

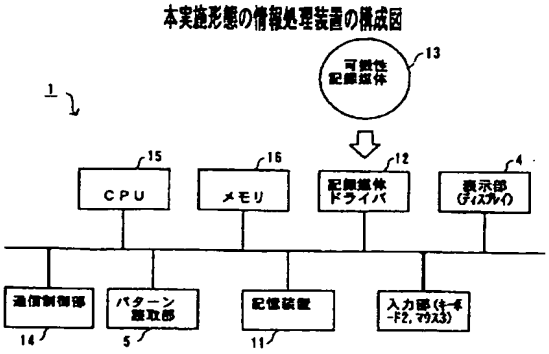
【図６】本実施形態の復号化処理のフローチャートである。

【図７】データ読み出し時に表示されるデータ一覧の例である。

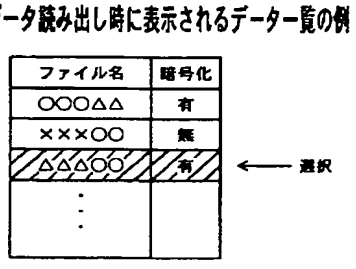
【符号の説明】

１	情報処理装置
２	キーボード
３	マウス
４	ディスプレイ
５	パターン読取部
１１	記憶装置
１２	記録媒体ドライバ
１３	可搬性記録媒体
１４	通信制御部
１５	ＣＰＵ
１６	メモリ

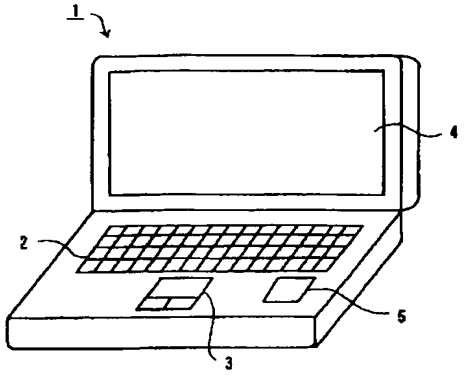
【図２】



【図７】

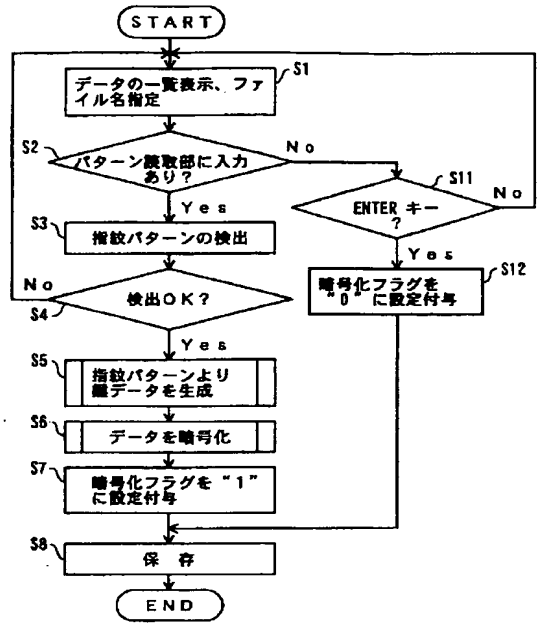


【図１】



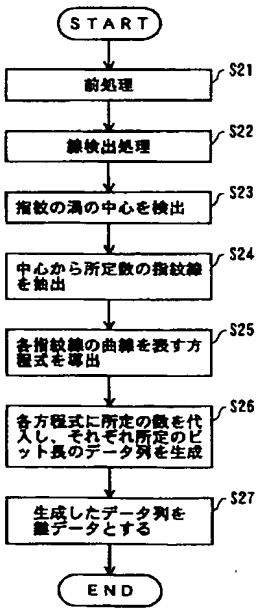
【図３】

本実施形態の暗号化処理のフローチャート



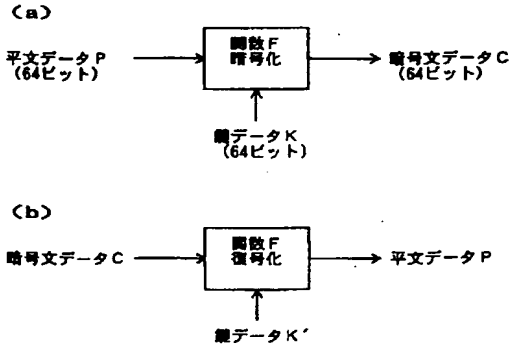
【図４】

指紋パターンに基づいて鍵データを生成する処理のフローチャート



【図５】

(a) および(b) はそれぞれ暗号化処理および復合化処理の概念を説明する図



【図６】

本実施形態の復号化処理のフローチャート